REMARKS

Applicant hereby cancels claim 18 without prejudice or disclaimer. Therefore, claims 1-14, 16, 17, 19 and 20 are all the claims pending in the application.

Claim Rejections - 35 U.S.C. § 103

Claims 1-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Van Buer (US 2003/0198345) in view of Takagi et al. (US 6,259,790), hereinafter "Takagi". Applicant submits the following in traversal.

Claim 1

The Examiner, in the Final Office Action dated December 16, 2009, correctly concedes that Van Buer does not explicitly disclose a coefficient table providing first to fourth coefficients in response to said row index, but cites Takagi to make up for the deficiency (Fig. 13 and col. 26, lines 54-67 to col. 27, lines 1-5 of Takagi). Specifically, Takagi discloses a coefficient calculation unit 137a (see Fig. 13) which outputs coefficients K_0, $K_1 \ldots K_{k-1}$. It appears that the Examiner is contending that the coefficient table memory unit 137c (shown inside the coefficient calculation unit 137a in Fig. 13 of Takagi) corresponds to the claimed coefficient table. Assuming *arguendo* that such a correspondence can be made, Applicant submits that the combination of the teachings of Van Buer and Takagi fails to disclose or suggest at least "first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively" for at least the following reasons.

In a non-limiting embodiment of the present invention, a row multiplexer 104 and a column multiplexer 102 are used to select a requested element from the input state 101 and provide the selected element for the S-box 105 (see page 28, lines 5-25 of the originally filed specification). Further, in a non-limiting embodiment of the present invention, a substitution value obtained from the S-box, with respect to the selected element, is provided for the first to fourth Galois field multipliers 107_0 to 107_3, where the products of the substitution value and coefficients d_0 to d_3 received from a coefficient table 106 are computed (see page 29, lines 7-13 and page 30, lines 9-13 of the originally filed specification). Claim 1 reflects these features by reciting "first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively".

On the contrary, Van Buer discloses a bitwise exclusive or (x-or) operation between a round key and data before providing the output of the x-or operation to substitution (see Fig. 2 of Van Buer). As noted in the response dated March 16, 2010, Applicant submitted that the x-or operation of Van Buer is defined as an add operation and not a multiplication operation. Further, it is also noted that the x-or operation of Van Buer is performed before providing a value to the S-box (see Fig. 24: for encryption and decryption, the x-or operations (778 and 782) are performed before providing a value to the S-box 802). On the other hand, as noted above, claim 1 recites "first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients,

respectively". Therefore, the x-or operation of Van Buer cannot correspond to the claimed multiplication of said substitution value with the first to fourth coefficients.

Furthermore, in Fig. 13, Van Buer discloses that each octet W1, W2, W3 and W4 is transformed (multiplied) by, respectively, operations x2 and x3 in GF (2^n). In other words, Van Buer discloses a mixing logic that can be utilized in encryption (paragraph [0077]). However, the multiplication of each of the octets W1, W2, W3 and W4 with the operations x2 and x3 is performed before providing a value to the S-box. Specifically, in Fig. 24, Van Buer clearly discloses a Mix operation 776 before providing a value to the S-box 802 (see also paragraph [0086] of van Buer). On the other hand, as noted above, claim 1 recites "first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively". Therefore, even if the Examiner is intending to argue that the Mix operation 776 of Van Buer corresponds to the claimed multiplication of said substitution value with the first to fourth coefficients, Applicant submits that such a correspondence cannot be made at least in view of the above.

In view of the foregoing, even if a combination is made to modify the teachings of Van Buer by a coefficient table memory unit 137c of Takagi providing coefficients, Applicant submits that the combination, at most, would result in providing coefficients during the Mix operation 776 stage for multiplication of the octets W2, W2, W3 and W4 of Van Buer (as shown in Fig. 13 of Van Buer) with the coefficients of Takagi. As such, the above noted combination of Van Buer and Takagi, at most, would disclose multiplication of the octets W2, W2, W3 and W4 of Van Buer (as shown in Fig. 13 of Van Buer) with the coefficients of Takagi before

providing a value to the S-box 802 of Van Buer. Van Buer and Takagi, alone or in combination, fail to disclose or suggest multiplying coefficients with the output of the S-box disclosed by Van Buer. Therefore, the combination of Van Buer and Takagi fails to disclose or suggest at least "first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively".

In view of the above, Applicant respectfully submits that claim 1 is not rendered unpatentable.

For reasons similar to those submitted for claim 1, Applicant respectfully submits that claims 3, 6, 8, 11, 12 and 14 are not rendered unpatentable.

Claims 2, 4, 5, 7, 9, 10, 13, 16, 17, 19 and 20, which depend from claims 1, 3, 6, 8 or 12, are not rendered unpatentable at least by virtue of their dependencies.

Claim 18 is canceled without prejudice or disclaimer, as noted above. Accordingly, Applicant submits that the rejection of claims 18 under § 103(a) is moot.

Further, as noted in the Response dated March 16, 2010, the Examiner fails to address the features of claims 2, 4, 5, 7, 9, 10, 13 and 16-20. According to 37 C.F.R. § 1.104(c), Applicant notes that in rejecting claims for want of novelty or for obviousness, the pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. Since the Examiner has failed to specify each rejected claim, in addition to be patentable by virtue of their dependencies, Applicant maintains that claims 2, 4, 5, 7, 9, 10, 13 and 16, 17, 19 and 20 are allowable.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/J. Warren Lytle, Jr./

J. Warren Lytle, Jr.
Registration No. 39,283

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: April 16, 2010